

REMARKS

Prior to entry of this amendment, claims 1-5, 7-18, and 20-25 are currently pending in the subject application. Claims 1, 12, 21 and 23 are independent.

By the instant amendment, claims 1, 7, 12, and 21-23 have been amended, as supported at least by paragraph [0027] of the Application Publication. No new matter has been added.

A. Introduction

In the outstanding Office action,

- a) claims 23-25 were objected to because of language informalities;
- b) claims 1-5, 7-18, and 20-25 were rejected under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicants regard as the invention;
- c) claims 1-5, 8-18, 21 and 23-25 were rejected under 35 U.S.C. § 103(a) as being unpatentable over “Key Agreement in ad hoc Networks,” *Computer Communications*, Volume 23, Number 17, 1 November 2000 to Asokan et al. (“the Asokan et al. reference”) in view of “Handbook of Applied Cryptography”, CRC Press, pp. 551-553, (10-1996) to Menezes et al. (“the Menezes et al. reference”);
- d) claims 7, 20 and 22 were rejected under 35 U.S.C. § 103(a) as being unpatentable over the Asokan et al. reference – Menezes et al. reference in further view of “Applied Cryptography” second edition, 1996 to Schneier (“the Schneier reference”);
- e) claims 1-5, 8-18, 21 and 23-25 were rejected under 35 U.S.C. § 103(a) as being unpatentable over “the Asokan et al. reference in view of U.S. Patent Publication No. 2003/0210787 to Billhartz et al. (“the Billhartz et al. reference”);
- f) claims 7, 20 and 22 were rejected under 35 U.S.C. § 103(a) as being unpatentable over the Asokan et al. reference – Billhartz et al reference in further view of the Schneier reference;
- g) claims 1-5, 8-18, 21 and 23-25 were rejected under 35 U.S.C. § 103(a) as being unpatentable over “the Asokan et al. reference in view of U.S. Patent No. 6,889,321 to Kung et al. (“the Kung et al. reference”); and
- h) claims 7, 20 and 22 were rejected under 35 U.S.C. § 103(a) as being unpatentable over the Asokan et al. reference – Kung et al reference in further view of the Schneier reference.

B. Objection to Claims 23-25

In the outstanding Office action, claims 23-25 were objected to because of language informalities. By the instant amendment, claim 23 has been amended to clarify language pointed out by the Examiner. Therefore, it is requested that this objection be withdrawn.

C. Asserted Indefiniteness Rejection of Claims 1-5, 7-18, and 20-25

In the outstanding Office action, claims 1-5, 7-18, and 20-25 were rejected under 35 U.S.C. § 112, second paragraph. By the instant amendment, claims 1, 12, 21, and 23 have been amended to clarify allegedly unclear language pointed out by the Examiner. Therefore, it is requested that this rejection be withdrawn.

D. Asserted Obviousness Rejections of Claims 1-5, 7-18, and 20-25

In the outstanding Office action, claims 1-5, 8-18, 21 and 23-25 were rejected under 35 U.S.C. § 103(a) as being unpatentable over the Asokan et al. reference in view of the Menezes et al. reference, and claims 7, 20 and 22 were rejected under 35 U.S.C. § 103(a) as being unpatentable over the Asokan et al. reference – Menezes et al. reference further in view of the Schneier reference. These rejections are traversed for at least the reasons set forth below.

Independent claim 1 has been amended to clarify and recite, *inter alia*,

transmitting the at least one modified second group key to the (N-1) sub wireless terminals using the initial second group key, wherein the at least one modified second group key is transmitted and used to encode data between the N wireless terminals during use of the first group key.

Independent claims 12, 21, and 23 have been amended to include language parallel to the amendatory language of claim 1. Applicants respectfully submit that neither the Asokan et al. reference nor the Menezes et al. reference, whether alone or in any combination, teach or even remotely suggest transmission of a modified second group key as currently recited in independent claims 1, 12, 21 and 23. In particular, the cited references do not teach that at

least one modified second group key, which is transmitted using the initial second group key, is transmitted and used during use of the first group key. In other words, the cited references do not teach, *inter alia*, using at least one modified second group key, including an *overlapping use of the initial second group key and modified second group key*, during use of the first group key.

Further, applicants disagree with the interpretation in the outstanding Office action that since “a session key in the Asokan et al reference is for [] fixed periods (i.e. session) and [is replaced, while] the password (i.e., first group key) is always present,” the Asokan et al reference teaches the features recited in claims 1, 12, 21, and 23.¹ Applicants respectfully point out that the Asokan et al. reference teaches both a “session key” and a password that are static and are generated specifically for a single communication session.² For example, if a P5 session key of the Asokan et al. reference is used with a first password in a first communication session, the P5 session key is modified only for use in a second communication session having a second password. Accordingly, the modified P5 session key of the Asokan et al. reference cannot be used during use of the first password. Applicants respectfully submit that the Menezes et al. reference fails to teach or even remotely suggest this deficiency of the Asokan et al. reference.

As an additional matter, with respect to the rejection of claims 7, 20, and 22, applicants respectfully point out that, contrary to the assertion on page 13 of the outstanding Office action, the Schneier reference does not teach *encoding and transmitting* a modified key with an initial key. In particular, the Schneier reference merely teaches updating a key, i.e., use portions of a first key to *generate* a second key.³ Since “generation” of a key is defined as -- bringing into being of a key --, “encoding” of a key is defined as --putting a key

¹ Office action of July 7, 2008, page 8, lines 17-20.

² Applicants note the second full paragraph on page 7 of the Asokan et al. reference, which indicates that a fresh keypair is preferred for each run of a protocol.

³ The Schneier reference, Section 8.6, line 6.

into a code,-- and “transmitting” a key is defined as -- sending or conveying a key,⁴-- generation of a second key using a first key as taught by the Schneier reference does not teach the limitations of claims 7, 20, and 22.

It is respectfully submitted that the Asokan et al. reference and the Menezes et al. reference, whether alone or in combination, fail to disclose or suggest the subject matter recited in independent claims 1, 12, 21, and 23. The remaining rejected claims depend, either directly or indirectly, from respective ones of these independent claims, and are believed to be allowable for at least the reasons their respective base claims are believed to be allowable. Therefore, it is respectfully requested that this rejection be withdrawn.

E. Asserted Obviousness Rejections of Claims 1-5, 7-18, and 20-25

In the outstanding Office action, claims 1-5, 8-18, 21 and 23-25 were rejected under 35 U.S.C. § 103(a) as being unpatentable over the Asokan et al. reference in view of the Billhartz et al. reference, and claims 7, 20 and 22 were rejected under 35 U.S.C. § 103(a) as being unpatentable over the Asokan et al. reference – Billhartz et al. reference further in view of the Schneier reference. These rejections are traversed for at least the reasons set forth below.

Applicants respectfully submit that the Billhartz et al. reference fails to teach or even remotely suggest features missing from the Asokan et al. reference, which were discussed in detail previously, i.e., in section D above. In particular, the Billhartz et al. reference does not teach that at least one modified second group key, which is transmitted using the initial second group key, is transmitted and used during use of the first group key. Therefore, it is respectfully submitted that claims 1, 12, 21, and 23 are allowable for at least the reasons discussed previously in section D above. The remaining rejected claims depend, either directly or indirectly, from respective ones of these independent claims, and are believed to

⁴ The American Heritage Dictionary.

be allowable for at least the reasons their respective base claims are believed to be allowable.

Therefore, it is respectfully requested that this rejection be withdrawn.

F. Asserted Obviousness Rejection of Claims 1-5, 7-18, and 20-25

In the outstanding Office action, claims 1-5, 8-18, 21 and 23-25 were rejected under 35 U.S.C. § 103(a) as being unpatentable over the Asokan et al. reference in view of the Kung et al. reference, and claims 7, 20 and 22 were rejected under 35 U.S.C. § 103(a) as being unpatentable over the Asokan et al. reference – Kung et al. reference further in view of the Schneier reference. These rejections are traversed for at least the reasons set forth below.

Applicants respectfully submit that the Kung et al. reference fails to teach or even remotely suggest features missing from the Asokan et al. reference, which were discussed in detail previously, i.e., in section D above. In particular, the Kung et al. reference does not teach that at least one modified second group key, which is transmitted using the initial second group key, is transmitted and used during use of the first group key. Therefore, it is respectfully submitted that claims 1, 12, 21, and 23 are allowable for at least the reasons discussed previously in section D above. The remaining rejected claims depend, either directly or indirectly, from respective ones of these independent claims, and are believed to be allowable for at least the reasons their respective base claims are believed to be allowable. Therefore, it is respectfully requested that this rejection be withdrawn.

G. Conclusion

The above remarks demonstrate failings of the rationales underlying the outstanding rejections, and are sufficient to overcome the outstanding rejections. However, these remarks are not intended to, nor need they, comprehensively address each and every reason for the patentability of the claimed subject matter over the applied art. Accordingly, applicants submit that the claims are allowable for reasons including, but not limited to, those set forth

above, and patentability of the claims does not depend solely on the particular claim element discussed above.

The remaining documents cited in the Office action were not relied on to reject the claims. Therefore, no comments concerning these documents are considered necessary at this time.


In view of the foregoing amendments and remarks, reconsideration of this application is earnestly solicited, and an early and favorable further action upon all the claims is hereby requested.

If the Examiner believes that additional discussions or information might advance the prosecution of the instant application, the Examiner is invited to contact the undersigned at the telephone number listed below to expedite resolution of any outstanding issues.

Respectfully submitted,

LEE & MORSE, P.C.

Date: November 6, 2008



Lilia C. Lord, Reg. No. 58,420

LEE & MORSE, P.C.
3141 FAIRVIEW PARK DRIVE, SUITE 500
FALLS CHURCH, VA 22042
703.207.0008 TEL
703.207.0003 FAX

PETITION and
DEPOSIT ACCOUNT CHARGE AUTHORIZATION

This document and any concurrently filed papers are believed to be timely. Should any extension of the term be required, applicant hereby petitions the Director for such extension and requests that any applicable petition fee be charged to Deposit Account No. 50-1645.

If fee payment is enclosed, this amount is believed to be correct. However, the Director is hereby authorized to charge any deficiency or credit any overpayment to Deposit Account No. 50-1645.

Any additional fee(s) necessary to effect the proper and timely filing of the accompanying-papers may also be charged to Deposit Account No. 50-1645.